Datenschutzrichtlinie der LSB Thüringen Bildungswerk GmbH

§ 1 Bedeutung, Ziel, Zugänglichkeit

(1) Diese Richtlinie ist die verbindliche Basis für einen rechtskonformen und nachhaltigen Schutz personenbezogener Daten in der LSB Thüringen Bildungswerk GmbH (BW).
(2) Mit dieser Richtlinie sollen die Persönlichkeitsrechte von Betroffenen gewahrt und geschützt werden.
(3) Die Richtlinie muss für alle Beschäftigten und leitenden Angestellten jederzeit leicht zugänglich sein.

§ 2 Geltungsbereich

(1) Diese Richtlinie findet Geltung für die LSB Thüringen Bildungswerk GmbH.
(2) Sie gilt für alle Beschäftigten sowie leitenden Angestellten des BW.
(3) Die Gebote und Verbote dieser Richtlinie gelten für jeglichen Umgang mit personenbezogenen Daten, unabhängig ob dieser elektronisch oder in Papierform vonstattengeht. Ebenso beziehen sie alle Arten von Betroffenen (Mitglieder, Kunden, Gäste, Lieferanten, Beschäftigte etc.) in ihren Geltungsbereich ein.

§ 3 Begriffsbestimmungen

(1) **Personenbezogene Daten** sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Betroffener). Kundendaten gehören dabei ebenso zu den personenbezogenen Daten wie Personaldaten von Beschäftigten. Beispielsweise lässt der Name einer*s Ansprechpartner*in ebenso einen Rückschluss auf eine natürliche Person zu, wie seine*ihre E-Mail- Adresse. Es genügt, wenn die jeweilige Information mit dem Namen des*der Betroffenen verbunden ist oder unabhängig hiervon aus dem Zusammenhang hergestellt werden kann. Ebenso kann eine Person bestimmbar sein, wenn die Information erst mit einem Zusatzwissen verknüpft werden muss, so z. B. beim Autokennzeichen. Das Zustandekommen der Information ist für einen Personenbezug unerheblich. Auch Fotos, Video- oder Tonaufnahmen können personenbezogene Daten darstellen.
(2) **Besondere Arten personenbezogener Daten** sind Informationen, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen sowie eine eventuelle Gewerkschaftszugehörigkeit hervorgehen können sowie genetische Daten, biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben bzw. der sexuellen Orientierung einer natürlichen Person.
(3) **Verarbeitung** ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

auf folgender Grundlage erstellt und angepasst: Koreng/Lachenmann Datenschutz-R-FormHdB, II. Unternehmensrichtlinie Datenschutz für Mitarbeiter Rn. 1. – 21. beck-online

(4) **Einschränkung der Verarbeitung** ist die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.

(5) **Profiling** bezeichnet jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.

(6) **Pseudonymisierung** ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

(7) **Verantwortlicher** ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(8) **Auftragsverarbeiter** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(9) **Empfänger** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht.

(10) **Dritter** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

(11) Eine **Einwilligung des Betroffenen** ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der der Betroffene zu verstehen gibt, dass er mit der Verarbeitung der ihn betreffenden personenbezogenen Daten einverstanden ist.

§ 4 Datenschutzorganisation

(1) Das BW hat eine Datenschutzbeauftragte nach Maßgabe des Bundesdatenschutzgesetzes (BDSG) bestellt.

Diese erreichen Sie unter folgenden Kontaktdaten:

Susan Klimitsch
LSB Thüringen Bildungswerk GmbH
Fachkraft für Datenschutz
Tel. 0361-34054450
datenschutz@lsb-bildungswerk.de

(2) Die vorgenannte Person überwacht und gewährleistet die Einhaltung der DS-GVO, der gesetzlichen Vorgaben einschließlich der Vorgaben dieser und anderer Richtlinien des BW zum Datenschutz. Sie berät die Geschäftsführung zu Fragen des Datenschutzes, ist zuständig bei der Kommunikation mit Betroffenen und Aufsichtsbehörden und berichtet der Geschäftsführung regelmäßig über die Umsetzung des Datenschutzes in der BW. Sie berät sich bei Bedarf, entwickelt Konzepte zur Verbesserung des Datenschutzes und kontrolliert ausgewählte Prozesse stichprobenartig und in angemessenen Zeitabständen auf ihre Datenschutzkonformität.
Die Datenschutzbeauftragte nimmt ihre Aufgaben weisungsfrei und unter Anwendung ihrer Fachkunde wahr.

(3) Die BW bzw. ihre Mitarbeiter*innen unterstützen die Datenschutzbeauftragte bei der Erfüllung ihrer Aufgaben.

(4) Bei der Konzeption neuer Projekte, bei denen personenbezogene Daten verarbeitet werden, ist die Datenschutzbeauftragte einzubinden.

§ 5 Umgang mit personenbezogenen Daten

(1) Die Verarbeitung von personenbezogenen Daten ist grundsätzlich verboten, es sei denn eine gesetzliche Norm erlaubt explizit den Datenumgang. Personenbezogene Daten dürfen nach der DS-GVO grundsätzlich verarbeitet werden:

- Bei einem bestehenden Vertragsverhältnis mit dem Betroffenen. Beispiel: Die Speicherung und Verwendung erforderlicher personenbezogener Daten im Rahmen eines Arbeitsverhältnisses oder Mitgliedsverhältnisses.
- Im Zuge vorvertraglicher Maßnahmen auf Anfrage des Betroffenen sowie der Vertragsabwicklung mit dem Betroffenen soweit die Verarbeitung dazu erforderlich ist. Beispiel: Ein Mitglied fordert Informationen zu einer Veranstaltung an und meldet sich zu dieser an oder ein Gast bucht ein Zimmer. Die erforderlichen Daten zur Zusendung des Anmelde- und / oder Informationsmaterials sowie zur Abwicklung der Veranstaltung (z.B. Bestätigung der Teilnahme sowie Zahlung der Gebühr) dürfen erhoben und verarbeitet werden.
- Wenn und soweit der Betroffene eingewilligt hat. Beispiel: Das Mitglied stimmte der Zusendung weiteren Informationsmaterials zu.
- Wenn berechtigte Interessen des Verantwortlichen (LSB e.V. oder die Gesellschaften) bestehen, sofern nicht die Interessen oder Grundrechte des Betroffenen überwiegen, insbesondere wenn es sich um ein Kind handelt. Datenverarbeitungen unter Berufung auf ein berechtigtes Interesse sollten jedoch nicht ohne vorherige Beratung durch die Datenschutzbeauftragte vorgenommen werden.
- Wenn eine rechtliche Verpflichtung besteht, der LSB e.V. und/oder der Gesellschaften unterliegt. Beispiel: Gesetzliche Aufbewahrungsfristen nach Handelsgesetzbuch (HGB) und Abgabenordnung (AO).

(2) Betroffene dürfen nicht einer ausschließlich auf einer automatisierten Verarbeitung – so auch dem Profiling – beruhenden Entscheidung unterworfen werden, die ihnen gegenüber eine rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

(3) Personenbezogene Daten sind für einen zuvor festgelegten, eindeutigen und legitimen Zweck zu verarbeiten. Eine Datenhaltung ohne Zweck, so beispielsweise die Speicherung von Daten auf Vorrat, ist unzulässig.

(4) Soweit möglich, sollte auf einen personenbezogenen Datenumgang verzichtet werden. Pseudonyme oder anonyme Datenverarbeitungen sind vorzuziehen. Beispielsweise kann es im Rahmen einer statistischen Auswertung von Daten nicht notwendig sein, den Vollnamen eines Betroffenen zu kennen und zu verwenden. Vielmehr kann diese Information durch einen Zufallswert ersetzt werden, der eine Unterscheidbarkeit der zugrundeliegenden Information ebenfalls gewährleisten kann.

(5) Die Änderung einer Ziel- und Zweckbestimmung, die einer Datenverarbeitung ursprünglich zugrunde gelegt wurde, ist – neben der erklärten Einwilligung durch den Betroffenen – nur zulässig, wenn der Zweck der Weiterverarbeitung mit dem ursprünglichen Zweck vereinbar ist. Hierbei sind insbesondere die vernünftigen Erwartungen des Betroffenen hinsichtlich einer solchen Weiterverarbeitung gegenüber dem LSB e.V. und / oder der Gesellschaften, die Art der verwendeten Daten, die Folgen für den Betroffenen sowie Möglichkeiten einer Verschlüsselung oder Pseudonymisierung zu berücksichtigen.

(6) Der Betroffene ist bei der Erhebung seiner personenbezogenen Daten umfassend über den Umgang mit seinen Daten zu informieren. Die Information hat die Zweckbestimmung, die Identität der verantwortlichen Stelle, die Empfänger seiner personenbezogenen Daten sowie alle sonstigen Information im Sinne des Art. 13 DS-GVO zu beinhalten, um eine faire und transparente Verarbeitung zu gewährleisten. Die Information ist in einer verständlichen und leicht zugänglichen Form sowie einer möglichst einfachen Sprache zu verfassen.

(7) Werden personenbezogene Daten nicht beim Betroffenen erhoben, sondern werden beispielsweise bei einer anderen Mitgliedsorganisation beschafft, ist der Betroffene nachträglich und umfassend gem. Art. 14 DS-GVO über den Umgang mit seinen Daten zu informieren. Dies gilt auch für die Änderung einer Ziel- und Zweckbestimmung der Datenverarbeitung.

(8) Personenbezogene Daten müssen sachlich richtig und auf dem neusten Stand sein. Der Umfang der Datenverarbeitung sollte hinsichtlich der festgelegten Zweckbestimmung erforderlich und relevant sein. Der jeweilige Geschäftsbereich, die jeweilige Abteilung bzw. Betriebstätte hat für die Umsetzung durch die Etablierung entsprechender Prozesse Sorge zu tragen. Ebenso sind Datenbestände regelmäßig auf ihre Richtigkeit, Erforderlichkeit und Aktualität hin zu überprüfen.

§ 6 Besondere Kategorien personenbezogener Daten

Besondere Kategorien personenbezogene Daten dürfen grundsätzlich nur mit Einwilligung des Betroffenen oder ausnahmsweise aufgrund einer expliziten gesetzlichen Erlaubnis erhoben, verarbeitet oder genutzt werden. Ferner sind zusätzliche technische und organisatorische Maßnahmen (z. B. Verschlüsselung beim Transport, minimale Rechtevergabe) zum Schutz besonderer personenbezogener Daten zu ergreifen.

§ 7 Datenübermittlung/Datenweitergabe

(1) Die Übermittlung von personenbezogenen Daten an Dritte ist nur aufgrund gesetzlicher Erlaubnis oder der Einwilligung des Betroffenen zulässig.

(2) Befindet sich der Empfänger personenbezogener Daten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums bedarf es besonderer Maßnahmen zur Wahrung von Rechten und Interessen Betroffener. Eine Datenübermittlung ist zu unterlassen, wenn bei der empfangenden Stelle kein angemessenes Datenschutzniveau vorhanden ist oder beispielsweise über besondere Vertragsklauseln nicht hergestellt werden kann.

§ 8 Externe Dienstleister

(1) Sofern externe Dienstleister Zugriff auf personenbezogene Daten erhalten sollen, ist die Datenschutzbeauftragte vorab zu informieren.

(2) Dienstleister mit einem möglichen Zugriff auf personenbezogene Daten sind vor der Auftragserteilung sorgfältig auszuwählen. Die Auswahl ist zu dokumentieren und sollte insbesondere die folgenden Aspekte berücksichtigen:
- Fachliche Eignung des Auftragnehmers für den konkreten Datenumgang
- Technisch-organisatorische Sicherheitsmaßnahmen
- Erfahrung des Dienstleisters im Markt
- Sonstige Aspekte, die auf eine Zuverlässigkeit des Dienstlesiters schließen lassen (Datenschutz-Dokumentationen, Kooperationsbereitschaft, Reaktionszeiten etc.)

(3) Soll ein Dienstleister personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen, bedarf es des Abschlusses eines Vertrags zur Auftragsverarbeitung. Hierin sind Datenschutz- und IT-Sicherheitsaspekte zu regeln.

(4) Der Dienstleister ist im Hinblick auf die mit ihm vertraglich vereinbarten technisch-organisatorischen Maßnahmen regelmäßig zu überprüfen. Das Ergebnis ist zu dokumentieren.

§ 9 Datenvermeidung, Datensparsamkeit, Privacy by Default (Datenschutz durch Technikgestaltung)

(1) Der Umgang mit personenbezogenen Daten ist an dem Ziel auszurichten, so wenige Daten wie möglich von einem Betroffenen zu erheben und zu

verarbeiten (Datenminimierung). Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem

Verwendungszweck möglich ist.

(2) Entsprechendes gilt für die Auswahl und Gestaltung von Datenverarbeitungs-systemen. Der Datenschutz ist von Anfang an in die Spezifikationen und die Architektur von Datenverarbeitungssystemen zu integrieren, um die Einhaltung der Grundsätze des Schutzes der Privatsphäre und des Datenschutzes durch Technikgestaltung zu erleichtern („Privacy by design“) und den Grundsatz der Datenminimierung konsequent zu verfolgen.

§ 10 Rechte von Betroffenen

(1) Betroffene haben das Recht auf Auskunft über die im Unternehmen über ihre Person gespeicherten personenbezogenen Daten.

(2) Bei der Bearbeitung von Anträgen ist die Identität des Betroffenen zweifelsfrei festzustellen. Bei begründeten Zweifeln an der Identität können zusätzliche Angaben vom Antragsteller angefordert werden.

(3) Die Auskunftserteilung erfolgt schriftlich, es sei denn der Betroffene hat den Antrag auf Auskunft elektronisch gestellt. Der Auskunft ist eine Kopie der Daten des Betroffenen beizufügen, die, neben den zur Person vorhandenen Daten, auch die Empfänger von Daten, den Zweck der Speicherung sowie alle weiteren gesetzlich geforderten Informationen nach Art. 15 DS-GVO beinhaltet, um den Betroffenen die Verarbeitung bewusst zu machen und die Rechtmäßigkeit selbst beurteilen zu lassen. Auf besonderen Wunsch des Betroffenen werden die Daten in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt. Die zuständige IT-Abteilung legt den hierfür vorzusehenden Standard fest.

(4) Betroffene haben einen Anspruch auf Berichtigung ihrer personenbezogenen Daten, wenn sich diese als unrichtig erweisen. Ebenso können sie die Vervollständigung unvollständiger personenbezogener Daten verlangen.

(5) Der Betroffene hat das Recht auf Löschung seiner personenbezogenen Daten unter den folgenden Voraussetzungen:
- die Kenntnis der Daten ist für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich,
- der Betroffene hat eine Einwilligung widerrufen und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung,
- ihre Verarbeitung ist unzulässig,
- der Betroffene legt Widerspruch gegen die Verarbeitung zu Werbezwecken ein oder beruft sich auf ein Widerspruchsrecht aufgrund einer besonderen – zu begründenden – persönlichen Situation,
- es handelt sich um besondere personenbezogene Daten, deren Richtigkeit nicht bewiesen werden kann, oder
- es besteht eine anderweitige rechtliche Verpflichtung zur Datenlöschung.

Besteht eine Verpflichtung zur Löschung und wurden die personenbezogenen Daten zuvor öffentlich gemacht, sind weitere Verantwortliche für die Datenverarbeitung über ein Löschbegehren des Betroffenen hinsichtlich aller Kopien seiner Daten sowie aller Links zu diesen Daten zu informieren.

(6) Der Betroffene kann die Einschränkung der Verarbeitung seiner Daten verlangen, wenn
- die Richtigkeit der personenbezogenen Daten strittig ist, jedoch nur so lange, wie die Richtigkeit durch die zuständige Fachabteilung überprüft wird oder
- die Verarbeitung unzulässig ist, der Betroffene die Datenlöschung aber ablehnt, oder
- das Unternehmen die personenbezogenen Daten für Zwecke der Verarbeitung nicht mehr benötigt, der Betroffene die Daten jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, oder
- der Betroffene Widerspruch gegen die Verarbeitung aufgrund einer

besonderen Situation eingelegt hat und die zuständige Fachabteilung noch mit der Prüfung des Widerspruchs befasst ist.

(7) Der Betroffene ist spätestens innerhalb eines Monats über alle ergriffenen Maßnahmen, die auf seinen Antrag hin erfolgt sind, zu informieren.

(8) Die Datenschutzbeauftragte steht bei der Wahrung der Betroffenenrechte beratend zur Verfügung.

§ 11 Auskunftsersuchen Dritter über Betroffene

Sollte eine Stelle Informationen über Betroffene fordern, so beispielsweise Beschäftigte der BW ist eine Weitergabe von Informationen nur zulässig, wenn

- die Auskunft gebende Stelle ein berechtigtes Interesse hierfür darlegen kann, und
- das Auskunftsverlangen mit einer gesetzlichen Erlaubnisnorm im Einklang steht, sowie
- die Identität des Anfragenden oder der anfragenden Stelle zweifelsfrei feststeht.

§ 12 Verzeichnis von Verarbeitungstätigkeiten

(1) Die BW hat Verzeichnisse über alle Datenverarbeitungen zu führen. Verantwortlich dafür ist die Geschäftsführung. Die Datenschutzbeauftragte kann zur Beratung hinsichtlich der gesetzlich geforderten Informationen hinzugezogen werden.

(2) Das Unternehmen stellt der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung. Zuständig hierfür ist die Datenschutzbeauftragte im Einvernehmen mit der Unternehmensleitung.

§ 13 Werbung

(1) Die werbliche Ansprache von Betroffenen per Brief, Telefon, Fax, oder E-Mail ist grundsätzlich nur zulässig, wenn der Betroffene zuvor in die Verwendung seiner Daten zu Werbezwecken eingewilligt hat.

(2) Ausnahmen sind nur beim Vorliegen einer Erlaubnisnorm zulässig. Bitte konsultieren Sie diesbezüglich die Datenschutzbeauftragte.

§ 14 Schulung

Beschäftigte, die ständig oder regelmäßig Zugang zu personenbezogenen Daten haben, solche Daten erheben oder Systeme zur Verarbeitung solcher Daten entwickeln, sind in geeigneter Weise über die datenschutzrechtlichen Vorgaben zu schulen. Die Datenschutzbeauftragte entscheidet über Form und Turnus der entsprechenden Schulungen.

§ 15 Datengeheimnis

(1) Beschäftigten ist es untersagt, personenbezogene Daten unbefugt zu erheben und zu verarbeiten. Sie sind vor Aufnahme ihrer Tätigkeit auf einen

vertrauensvollen Umgang mit personenbezogenen Daten zu verpflichten. Die Verpflichtung erfolgt im Rahmen einer mündlichen Unterweisung in Verantwortung der Geschäftsleitung und wird schriftlich unter Verwendung des hierzu vorgesehenen Formulars dokumentiert.

(2) Mitarbeiter*innen mit besonderen Geheimhaltungsverpflichtungen (z. B. Fernmeldegeheimnis nach § 88 TKG) werden von der Geschäftsleitung ergänzend darauf schriftlich verpflichtet.

§ 16 Beschwerden

(1) Jeder Betroffene hat das Recht, sich über eine Verarbeitung seiner Daten zu beschweren, sollte er sich hierdurch in seinen Rechten verletzt fühlen. Ebenso können Beschäftigte Verstöße gegen diese Unternehmensrichtlinie jederzeit anzeigen.

(2) Die zuständige Stelle für die oben genannten Beschwerden ist die Datenschutzbeauftragte als interne unabhängige und weisungsfreie Instanz.

§ 17 Prüfungen und Kontrollen

(1) Um ein hohes Datenschutzniveau zu gewährleisten, werden relevante Prozesse regelmäßig durch interne Stellen oder durch externe Kontrolleure überprüft. Im Falle der Feststellung eines Verbesserungspotentials sind unmittelbare Abhilfemaßnahmen zu treffen.

(2) Die bei der Prüfung gewonnenen Erkenntnisse sind zu dokumentieren. Die Dokumentation ist der Datenschutzbeauftragten und der Unternehmensleitung für den jeweiligen Prozess zu übergeben.

(3) Eine Prüfung ist erfolgreich abgeschlossen, wenn alle im Bericht dokumentierten Maßnahmen umgesetzt sind. Bei Bedarf werden Kontrollprüfungen durchgeführt, indem Empfehlungen des initialen Audits einer Überprüfung ihrer Implementierung unterzogen werden.

§ 18 Interne Ermittlungen

(1) Maßnahmen zur Sachverhaltsaufklärung und zur Vermeidung oder Aufdeckung von Straftaten oder schwerwiegenden Pflichtverletzungen im Arbeitsverhältnis sind unter genauer Beachtung der einschlägigen gesetzlichen Datenschutzvorschriften durchzuführen. Insbesondere müssen die dabei erhobenen und verwendeten Daten zum Erreichen des Ermittlungszwecks erforderlich, angemessen und mit Blick auf die schutzwürdigen Interessen der Betroffenen verhältnismäßig sein.

(2) Der Betroffene ist so bald wie möglich über die zu seiner Person durchgeführten Maßnahmen zu informieren.

(3) Bei allen Formen der internen Ermittlungen ist die Datenschutzbeauftragte hinsichtlich der Auswahl und Ausgestaltung der Maßnahmen vorab einzubeziehen

§ 19 Verfügbarkeit, Vertraulichkeit und Integrität von Daten

(1) In Abhängigkeit der Art der Daten und deren Schutzbedürftigkeit hat für jedes Verfahren eine dokumentierte Schutzbedarfsfeststellung und Risikoanalyse zu

erfolgen. Dies gilt insbesondere für besondere Kategorien personenbezogener Daten gem. § 6 dieser Richtlinie.

(2) Zur Wahrung der Verfügbarkeit, Vertraulichkeit und Integrität von Daten wird ein allgemeines Sicherheitskonzept erstellt, das für alle Verfahren verbindlich ist. Hierin sind insbesondere Mittel und Maßnahmen zur Verschlüsselung und Datensicherung vorzusehen.

(3) Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Bildschirme sind zu sperren. Türen unbesetzter Räume sind zu verschließen. Personenbezogene Daten in Papierform sind in verschlossenen Schränken bzw. Räumen aufzubewahren. Wirksame Maßnahmen zur Zugangskontrolle an Geräten müssen vorhanden und aktiviert sein. Systemzugänge sind in Abwesenheit stets zu sperren.

(4) Passwörter ermöglichen einen Zugang zu Systemen und den darin gespeicherten personenbezogenen Daten. Sie stellen eine persönliche Kennung des Nutzers dar und sind nicht übertragbar. Es ist sicherzustellen, dass Passwörter stets unter Verschluss gehalten werden. Sie müssen mindestens 8 Zeichen aufweisen und aus mindestens drei verschiedenen Zeichenarten bestehen Großbuchstaben, Kleinbuchstaben, Zahlen, Sonderzeichen). Die Gültigkeit der Passwörter ist zeitlich begrenzt. Passwörter dürfen nicht in einem Wörterbuch vorkommen oder aus leicht zu erratenden Begriffen gebildet werden, insbesondere nicht Begriffe, die im Zusammenhang mit dem Unternehmen stehen. Näheres regelt die Netzwerkrichtlinie.

(5) Zugriffe auf personenbezogene Daten sollen nur diejenigen Personen erhalten, die im Zuge ihrer Aufgabenwahrnehmung Kenntnis von den jeweiligen Daten erhalten müssen („Need-to-know-Prinzip“). Zugriffsberechtigungen müssen genau und vollständig festgelegt und dokumentiert sein.

(6) Datenübertragungen durch öffentliche Netze sind nach Möglichkeit zu verschlüsseln. Eine Verschlüsselung hat zwingend zu erfolgen, falls der Schutzbedarf der personenbezogenen Daten dies erfordert.

(7) Zu unterschiedlichen Zwecken erhobene personenbezogene Daten sind getrennt voneinander zu verarbeiten. Die Trennung von Daten ist durch geeignete technische und organisatorische Maßnahmen sicherzustellen.

(8) Wartungsarbeiten an Systemen oder Telekommunikationseinrichtungen durch externe Dienstleister sind zu beaufsichtigen. Ferner ist zu gewährleisten, dass Dienstleister nicht unbefugt auf personenbezogene Daten zugreifen können. Fernwartungszugänge sind nur im Einzelfall zu gewähren und müssen dem Prinzip der minimalen Rechtevergabe folgen. Fernwartungsaktivitäten sind nach Möglichkeit aufzuzeichnen oder zu protokollieren.

§ 20 Datenschutz-Folgenabschätzung

(1) Für Verfahren, für die, aufgrund der Datenverarbeitung, ein hohes Risiko für Rechte und Freiheiten von Betroffen zu erwarten ist, muss eine Datenschutz-Folgenabschätzung durchgeführt werden. Die Datenschutz-Folgenabschätzung enthält alle gesetzlich geforderten Beschreibungen des Art. 35 Abs. 7 DS-GVO.

(2) Die Datenschutzbeauftragte berät die Geschäftsführung bei der Durchführung der Datenschutz-Folgenabschätzung sowie bezüglich der Frage, wann Verarbeitungen ein hohes Risiko für Betroffene beinhalten

können.

§ 21 Verletzungen des Schutzes von Daten („Datenpanne“)

(1) Sollten personenbezogene Daten unrechtmäßig Dritten offenbart worden sein, sind darüber unverzüglich die Datenschutzbeauftragte, im Verhinderungsfall die Geschäftsleitung zu informieren. Diese entscheiden über das weitere Procedere.

(2) Die Meldung hat alle relevanten Informationen zur Aufklärung des Sachverhalts zu umfassen, insbesondere die empfangende Stelle, die betroffenen Personen sowie Art und Umfang der übermittelten Daten.

(3) Die Erfüllung einer etwaigen Informationspflicht gegenüber der Aufsichtsbehörde erfolgt ausschließlich durch die Datenschutzbeauftragte. Betroffene werden durch die Geschäftsleitung informiert, wobei die Datenschutzbeauftragte beratend hinzugezogen wird.

§ 22 Folgen von Verstößen

Ein fahrlässiger oder gar mutwilliger Verstoß gegen diese Richtlinie kann arbeitsrechtliche Maßnahmen nach sich ziehen, einschließlich einer fristlosen oder fristgerechten Kündigung. Ebenso kommen strafrechtliche Sanktionen und zivilrechtliche Folgen wie Schadenersatz in Betracht.

§ 23 Aktualisierung der Richtlinie

(1) Im Rahmen der Fortentwicklung des Datenschutzrechts sowie technologischer oder organisatorischer Veränderungen wird diese Richtlinie regelmäßig auf einen Anpassungs- oder Ergänzungsbedarf hin überprüft.

(2) Änderungen an dieser Richtlinie sind formlos wirksam. Die Beschäftigten sind umgehend und in geeigneter Art und Weise über die geänderten Vorgaben in Kenntnis zu setzen.

beschlossen am 01.09.2016 geändert (aktualisiert) zuletzt am 20.04.2023

auf folgender Grundlage erstellt und angepasst: Koreng/Lachenmann Datenschutz-R-FormHdB, II. Unternehmensrichtlinie Datenschutz für Mitarbeiter Rn. 1. – 21. beck-online